only for R_o cannot access privileges such as P_5, P_6, P_7, because these are labeled with compartments a, b, and c, while R_o has only compartment a. A user authorized for role R_1, or any role that inherits from R_1, can access P_5, P_6, P_7, because R_1 has compartments a, b, and c.

It will be apparent to those of skill in the art that for reasons of both cost and trust, it is desirable to build RBAC systems on a proven MLS operating system. From a cost standpoint, it will normally be much easier to build RBAC as a single trusted process, provide a trusted interface between RBAC and MLS to provide the mapping functions described above, and then rely on MLS to control access to objects, than to modify the kernel of a secure system or build a new one from the ground up. Trust and assurance may be even more important considerations. The assurance process for a secure computing system is lengthy and expensive. MLS systems on the market today have had extensive evaluations and years of use in the field, largely by military organizations. The addition of RBAC to these systems can make them much more useful for commercial applications. The method of the invention makes it possible to leverage the large investment in these systems to produce RBAC systems that are in demand for commercial use.

While a preferred embodiment of the invention has been described, it will be appreciated by those of skill in the art that further enhancements and modifications thereto are possible, specifically in connection with the assignment of compartments and levels to objects to be accessed via the RBAC interface. Many additional mapping schemes beyond those discussed above are within the scope of the invention. Accordingly, these and other modifications to the preferred embodiment disclosed herein are intended to be within the scope of the following claims where not specifically excluded thereby.

What is claimed is:

1. In a lattice-based multi-level security system of the type wherein each object to which access is controlled by said lattice-based multi-level security system is assigned to a compartment and level maintained thereby, and wherein individual subjects are permitted access to specified objects protected by said security system only if the particular subject possesses a clearance level at least equal to that assigned to the object, and if the object is assigned to a compartment authorized for use by the subject, a method of implementing role-based access control, comprising the following steps:

defining a collection of roles,

mapping each defined role to a set of privileges, each privilege providing access to one or more combinations of compartments and levels within said lattice-based multi-level security system,

assigning each subject to one or more of said roles, and

at the time a subject requests access to an object,

determining whether the subject is assigned to a role having privileges corresponding to the compartment and level of the requested object within said lattice-based multi-level security system, and

employing said lattice-based multi-level security system to control access of the subject to the object in response to said determination.

2. The method of claim **1**, wherein said step of determining whether the subject is assigned to a role having privileges corresponding to the compartment and level of the requested object within said lattice-based multi-level security system is performed by:

(1) determining the compartment and level of the requested object within said lattice-based multi-level security system,

(2) determining whether the subject belongs to a role mapped to a privilege providing access to the compartment and level of the requested object, and, if so,

(3) assigning the subject access to objects having compartments and levels equal to those of the requested object.

3. The method of claim **1**, comprising the further step of dividing the totality of compartments within said lattice-based multi-level security system into a first set of compartments that may be mapped to one or more of said collection of roles, and a second set of compartments that can not thus be mapped.

4. The method of claim **1**, comprising the further step of dividing the totality of levels supported by said lattice-based multi-level security system into a first set of levels that may be mapped to one or more of said collection of roles, and a second set of levels that can not thus be mapped.

5. The method of claim **1**, wherein as a new object is made available for access by said role-based access control method, said object is assigned to one or more compartments and levels within said lattice-based multi-level security system, and privileges providing access to said assigned compartments and levels are added to the set of privileges mapped to one or more of the defined roles.

6. The method of claim **1**, wherein said step of determining whether the subject is assigned to a role having privileges corresponding to the compartment and level of the requested object within said lattice-based multi-level security system is performed by:

assigning each defined role in a group of roles to a heirarchical tree, wherein a root role R_0 represents one or more privileges available to all roles in the group, and child nodes R_j can access all privileges associated with role R_j and any associated with roles R_i, where roles R_i are any ancestor nodes of R_j;

associating roles at level l of the tree, where n_l indicates the number of nodes at level l, with unique sets of compartments drawn from the set of remaining compartments;

choosing c compartments from the remaining set of compartments and removing these c compartments from the set of compartments available to designate roles; and

assigning a unique set of compartments to each privilege set at level l from the set of c compartments chosen.

* * * * *